



Key Establishment in TLS

Chris Hawk, chawk@certicom.com



TLS Protocols




certicom
encryption

- Handshake Protocol
- Alert Protocol
- Change Cipher Spec Protocol
- Application Data Protocol



Handshake Protocol

- Selects cipher suite
 - Exchanges authentication credentials
 - Establishes keys
- 



Key Exchange Mechanisms

- RSA/RSA Export
 - Diffie-Hellman
 - Elliptic Curve Diffie-Hellman
- 



Handshake Overview

Client Hello

List of cipher suites
Client Random Data

Server Hello

Selected cipher suite
Server Random Data

Server Certificate

X.509 Certificate chain

Server Key Exchange

If necessary

Client Key Exchange



Key Derivation

- Cipher suite key exchange method used to generate the master secret
- Key material derived through TLS Pseudo-Random Function (PRF)
- Inputs are Master Secret, Client Random, and Server Random



RSA Key Exchange

- Server sends its certificate containing RSA public key
- Client generates random key data, encrypts with server's public key



RSA Export Key Exchange

- Server send its RSA certificate
- Server generates 512 or 1024 bit key, signs and sends to the client
- Client encrypts random key data with ephemeral key



Ephemeral Diffie-Hellman

- Server sends certificate with DSA or RSA public key
- Server generates, signs and sends DH parameters and DH public value
- Client generates and sends DH public value




Static Diffie-Hellman

- Server sends RSA or DSA signed certificate containing DH parameters and public value
- Client generates and sends DH public value




Elliptic Curve Diffie-Hellman

- Server sends ECDSA signed certificate containing an EC public key
 - Client generates and sends an EC public key
- 



Final Key Derivation

- Pseudo-Random Function consists of HMAC-MD5 xor HMAC-SHA1
 - Final output of PRF is divided into key material for bulk cipher keys, MAC keys, and IVs
- 



Abbreviations

DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECDSA	Elliptic Curve DSA
DH	Diffie Hellman
TLS	Transport Layer Security

